Congress of the United States
Committee on International Relations
Subcommittee on Africa, Global Human Rights and International Operations

HEARING
The Internet in China: A Tool for Freedom or Suppression?

Wednesday, February 15, 2006 10:00 A.M.
Rayburn House Office Building, Room 2172

Testimony of Harry Wu
(Publisher, China Information Center)

First, I would like to thank Congressman Henry Hyde and Congressman Chris Smith for convening this hearing today on the important issue of Internet suppression in China. Thank you for your consistent support of the rights of the Chinese people and the work of organizations pushing for human rights in China.

In President Bush's speech in Kyoto during his recent trip to Asia, he urged China to take steps to promote freedom and democracy. What poses a challenge to freedom and democracy in China is not only the Beijing government, but also international companies that provide financial and technological assistance to the Beijing regime, allowing it to maintain its control.

It is common knowledge that a communist regime such as China's maintains total control over all forms of media- television, radio, newspaper and the Internet. The Chinese Communist Party has its own Propaganda Department, which ensures that all media content is consistent with official political doctrine. As technology has developed and expanded, the Chinese government has correspondingly developed and expanded its knowledge and its abilities to control it. As an example of this, there are currently at least 35,000 so-called "Internet police" in the Public Security Ministry whose job it is to monitor and censor websites and chatrooms in China.

From diplomacy and trade to strategic alliances and multilateral treaties, the last decade saw increased interaction and cooperation between the West and China. The outlook for liberalization was promising, despite China's notorious record of human rights abuses. Many argued that this type of "engagement" would lead the Chinese to a more liberal, democratic society. Others speculated that totalitarian regimes would only choke the liberating powers of the Internet. Unfortunately, current evidence suggests the pessimists are right. Censorship of the Internet is increasing with the explicit help of high-tech multilateral corporations. Beijing is seizing this opportunity to squash dissent and spy on its population with unparalleled efficiency.

While the introduction of technology into a society can be a positive force for change, it is important to consider the fact that technology can be used by all sides, and can therefore also be used as a negative force. In the current debate over the actions of American IT companies in China, these companies have asserted that they have provided the same technology and equipment that they have provided to all other countries they do business with. They maintain that they are not responsible for the ways in which their customers use the technology that they sell, and that they do not alter it in any ways to serve the needs of a particular customer, such as China's communist regime. They also argue that they are providing a positive service for the Chinese people by giving them technology and enabling them to have access to the outside world. But we must remember that this technology is like a pistol that can be used by all sides. While it can be used by the Chinese people, it can just as easily be used by the Chinese government to oppress them.

Information technology is often heralded as a tool to promote democracy, because it allows increased transparency and the liberalization of communication. But those living under authoritarian regimes cannot communicate with the world, or each other, freely- their right to privacy and free speech does not exist. China currently censors foreign and local media, and also suppresses dissent, but how far will China go in the name of "social stability"? Sadly, China is undertaking a monumental effort to monitor and track its citizens.

A friend of mine recently tried to access some politically sensitive websites while at an Internet café in a remote, small city in Xinjiang Province. The police quickly showed up to arrest him. I don't know who supplied the technology enabling the police to track my friend's Internet surfing, but I am pretty sure that U.S. technology was involved. The PRC's Ministry of Public Security has been continually upgrading and expanding its $800 million "Golden Shield" project- a government-sponsored surveillance system that was begun in 1998. The Golden Shield's advanced communication network was supposedly aimed at improving police effectiveness and efficiency. However, China has also used the "Golden Shield" as a way of monitoring Chinese civilians. The project will help prolong Communist rule by denying China's people the right to information. In order to develop the "Golden Shield," China has utilized the technologies of a number of foreign companies, such as Intel, Yahoo, Nortel, Cisco Systems, Motorola, and Sun Microsystems. The "Golden Shield Project" would not have been possible without the technology and equipment from these companies.

China has recently been clamping down hard on Internet cafés. Currently, everyone who wants to access the Internet at Internet cafés throughout China must register with their real names and present their identification card each time they come to surf the Net. This effectively prevents Internet users from even attempting to access any websites that the Chinese government deems inappropriate or politically sensitive. Government authorities throughout China have installed software in the computers in Internet cafés, enabling them to carry out comprehensive, long-term monitoring. This technological control software is capable of obtaining real-time information about

Internet users, and can also keep a record of instances in which Internet users exceed the Internet curfew.

While technology can be used to improve communications systems, it is clear that it can also be used for suppressive purposes. Today, the American IT companies that are present in China are working together with a totalitarian regime, that of the Chinese government. Therefore, despite the publicly-stated goals of these companies to provide Chinese people with greater information and access to the outside world, it is difficult for them to avoid working together with the immoral, corrupt Chinese regime.

Recently, there have been a number of cases in which Chinese "cyber-dissidents" have been sentenced to years in prison or placed under house arrest simply for sending e-mails or expressing their views online. China currently has the largest number of jailed Internet dissidents of any country in the world. From the following slides, we can learn about the cases of cyber-dissidents Huang Qi, Du Daobin, Shi Tao, and Liu Shui:

--On May 9, 2003, Huang Qi, founder and editor of the Tianwang website, was sentenced to five years' imprisonment for "subversion".

--Cyber-dissident Du Daobin was sentenced to four years of house arrest on June 11, 2004.

--In April 2005, journalist Shi Tao was sentenced to 10 years in prison for "divulging state secrets abroad".

--Cyber-dissident Liu Shui completed the two-year sentence of reeducation through labor which he received in 2004.

We now know that Yahoo complied with Chinese authorities in two separate incidents that resulted in the imprisonment of people for their activities on the Internet. Last week, it was reported that Yahoo released data that led to the arrest of Li Zhi, an online writer who was sentenced to eight years in prison in 2003, after posting comments that criticized official corruption. This case is parallel to that of Shi Tao, who was sentenced to 10 years in prison.

Moral responsibility for Yahoo's collaboration in the imprisonment of Li and Shi cannot be shrugged off with a simple assertion that Yahoo had no choice but to cooperate with Chinese authorities. A Yahoo spokeswoman insisted that in its dealings with China, the company "only responded with what we were legally compelled to provide, and nothing more". She argued that the company did not know how Chinese authorities would use the information it provided. However, we must ask who is making the laws and regulations requiring Yahoo to give up information about its customers. We must ask what kind of a government they are dealing with, and who they are providing a "pistol" to. The answer is that their major business partner is the Chinese government.

I would like to mention another example, involving the Beijing PKU High-Tech Fingerprint Co., Ltd., which collaborated with Intel Co. to greatly improve the speed of system operations, breaking through the limit of 100,000 prints per second. The capacity of the fingerprint database that was created exceeds 5,000,000. This fingerprint identification system is a part of the Public Security Bureau's (PSB) "Golden Shield Project", and is just one example of how the project is used to monitor and control Chinese citizens.

Similarly, Cisco Systems cannot dismiss criticism of its "Big Brother" censorship activities in China by maintaining that China's use of its equipment is beyond its control. Cisco Systems recently publicly confirmed that it has done business with China's PSB, and that it also provides service and training to its customers, who in this case they know are police officials. Cisco Systems, unlike other IT companies, has signed contracts *directly* with Chinese public security authorities.

Terry Alberstein, Director of Corporate Affairs for Cisco Systems - Asia Pacific, confirmed that Cisco does indeed sell networking and telecommunications equipment directly to Public Security and other law enforcement offices throughout China. According to Rconversation.com, the website of Rebecca MacKinnon, Alberstein said that Cisco sells to police around the world, and that it is not illegal for Cisco to do business with the Chinese police, because the equipment sold is not prohibited under the Foreign Relations Authorization Act. Mr. Alberstein reiterated that Cisco is doing nothing against U.S. law, and emphasized that Cisco does not tailor routers for the Chinese market and does not customize them for purposes of political censorship. According to Alberstein, "The products that Cisco sells in China are the same products we sell in the U.S. We do not custom-tailor any product for any export market." Also, an e-mail from Cisco Systems' public relations department that was also posted on Rconversation.com states that "Cisco Systems does not participate in the censorship of information by governments."

I'm glad Cisco has publicly confirmed that it has done business with China's Public Security Bureau, and that it also provides service and training to its customers. While Mr. Alberstein asserts that Cisco has not violated American law through its business dealings with the Chinese police, this is not up to Mr. Alberstein to decide. The U.S. Congress has the authority to decide if any violations have been committed. Cisco's technology and equipment have without question made the job of Chinese police easier and more effective. Cisco has assisted Chinese security forces with their monitoring capabilities, and Mr. Alberstein lacks the authority to say that this does not constitute crime control, which would be in violation of U.S. law.

Mr. Alberstein maintains that Cisco "sells networking equipment to law enforcement agencies around the world" and infers that its business activities in China are therefore identical to those in other countries. However, we are specifically talking about China, and there is a specific U.S. law that prohibits the export of crime control equipment to China. We should not believe the argument that Cisco's sales of high-tech equipment to China are as innocuous as such sales to some other countries, and we must

remember that there is a country-specific law in the Tiananmen Sanctions contained in Section 902(a)(4) of the Foreign Relations Authorization Act for Fiscal Year 1990-1991 (Public Law 101-246).

We should now ask Cisco to make public the information about exactly how much business it has done with China's PSB. Every Cisco shareholder has a right to know about this information. Cisco should publicize its profits, the quantity and date of its sales and business dealings, and its contacts in China, as well as the specific types of software and technology that have been sold. After Cisco has truthfully revealed this information, Congress and the American people can decide whether or not Cisco has committed a violation of the law.

Unfortunately, Cisco's sales pitch has been quite successful. Through several telephone inquiries to local managers of Cisco Systems in China, it was confirmed that nearly all of China has been employing Cisco's surveillance technology in provincial, district and county police agencies. Anyone departing from the Party line is considered a threat to "social stability." Cisco Systems' technology guarantees speech recognition, automated surveillance of telephone conversations, integration of biometric data, wireless Internet access to track individual users, video surveillance data from remote cameras back to a centralized surveillance point, etc. Indeed, the prospect of China's Golden Shield is unsettling for those for have worked so hard for a democratic China.

American law prohibits the export of devices that are to be used for "crime control", but perhaps we need to reevaluate the definition of a "crime control" device. Should this law apply only to metal handcuffs, or might it also apply to electronic handcuffs? Chinese citizens who were jailed for simply expressing their views online or for sending e-mails might have a different view about this definition. Manufacturers of handcuffs aren't allowed to sell their products to China's police, but Cisco and other companies are selling the Chinese authorities much more useful technology. U.S. export laws also ban the export of dual-use technology, and we may need to look at how "dual-use" is interpreted. When companies work together with the public security authorities of an oppressive regime, should we be concerned that the technology being provided will be used toward an evil purpose, and not just for its original purpose? I believe we should.

Selling advanced technology to China not only has strategic implications, it also prevents dissent and discussion that would otherwise play a positive role in reforming China's autocratic government. The U.S. spends millions of dollars to spread democracy. Why are we allowing American IT companies to undermine our message? Continued sales of high-tech equipment will strengthen China's ability to suppress democratic voices, and further tighten its grip over the Chinese population.

Attachment:
Slide captions

1. Notices from the Internet police can be seen everywhere in China.
2. Huang Qi, cyber- dissident, sentenced to five years' imprisonment.
3. Du Daobin, cyber-dissident, sentenced to four years' imprisonment.
4. Shi Tao, journalist, sentenced to 10 years' imprisonment.
5. Liu Shui, cyber-dissident, sentenced to two years of "reeducation through labor".
6. and 7. Beijing PKU High-Tech Fingerprint Co. cooperated with Intel, Sun Microsystems, Cisco, and Compaq.
8. Cisco builds up digital police power.
9. IP telephone and video solutions for police surveillance.
10. and 11. Cisco enhances the police force both scientifically and technologically.
12. Cisco's case study in Qinghai shows the expandability of its networking technology.
13. Cisco's technology is affordable for the Chinese police.
14. Cisco's case study in the Yunnan Police Department.
15. Cisco's case study of the IP digital network of the Beijing Police Bureau.
16. Strategic networking for the police.
17. The complete digitalized monitoring system.
18. Public Law 101-246 of the U.S. government.